(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
8 avril 2004 (08.04.2004)

PCT

(10) Numéro de publication internationale
WO 2004/030363 A1

(51) Classification internationale des brevets[7] :
H04N 7/167, 5/00

(21) Numéro de la demande internationale :
PCT/IB2003/004121

(22) Date de dépôt international :
19 septembre 2003 (19.09.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
2002 1623/02 27 septembre 2002 (27.09.2002) CH
2002 2048/02 4 décembre 2002 (04.12.2002) CH

(71) Déposant *(pour tous les États désignés sauf US)* : NAGRAVISION SA [CH/CH]; Route de Genève 22, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : NAHUM, Sylvain-Victor [FR/CH]; Avenue de l'Amandolier 24, CH-1208 Genève (CH). STRANSKY, Philippe [CH/CH]; Chemin des Grands-Champs, CH-1033 Cheseaux-sur-Lausanne (CH).

(74) Mandataire : LEMAN CONSULTING SA; Route de Clémenty 62, CH-1260 Nyon (CH).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: CONDITIONAL ACCESS DATA DECRYPTING SYSTEM

(54) Titre : SYSTÈME DE DÉCHIFFREMENT DE DONNÉES À ACCÈS CONDITIONNEL

(57) Abstract: The invention concerns a conditional access data decrypting system, in particular for use in pay digital television broadcast. Said system comprises a broadcasting center (1) designed to broadcast encrypted data by control words (cw), at least one management center (11) designed to broadcast personal messages (ECM, EMM) concerning access rights to the encrypted data and to manage said access rights, an operating device (12) for making said encrypted data usable, and a decoder (13) for decrypting at least part of the encrypted data. Said decoder is located between the broadcasting center (10) and the operating device (12). Said decoder (13) consists of a module for receiving (14) the encrypted data and a module for managing (15) access rights to said data. The reception module (14) is connected to or integral with the operating device (12) and the management module (15) is designed to communicate with the reception module. The management module (15) comprises a security module (16) designed to verify the content of the personal messages (ECM, EMM) and to allow or prevent decryption of the control words (cw) on the basis of the personal messages. The reception module receives the encrypted data from the broadcasting center (10) and the management module receives the enabling messages (EMM) from the management center (11).

(57) Abrégé : La présente invention concerne un système de déchiffrement de données ô accès conditionnel, en particulier utilisé dans le domaine de la télévision numérique ô péage. Ce système comporte un centre de diffusion (10) agencé pour diffuser des données chiffrées par des mots de contrôle (cw), au moins un centre de gestion (11) agencé pour diffuser des messages personnels (ECM, EMM) relatifs aux droits d'accès aux données chiffrées et pour gérer ces droits d'accès, un dispositif d'exploitation (12) destiné ô rendre utilisables lesdites données chiffrées, et un décodeur (13) agencé pour déchiffrer au moins une partie des données chiffrées. Ce décodeur est placé entre le centre de diffusion (10) et le dispositif d'exploitation (12). Ce décodeur (13) est formé d'un module de réception (14) des données chiffrées et d'un module de gestion (15) des droits d'accès ô ces données. Le module de réception (14) est connecté ou intégré au dispositif d'exploitation (12) et le module de gestion (15) est agencé pour communiquer avec le module de réception. Le module de gestion (15) comporte un module de sécurité (16) agencé pour vérifier le contenu des messages personnels (ECM, EMM) et pour permettre ou empêcher le déchiffrement des mots de contrôle (cw) en fonction du contenu des messages personnels. Le module de réception reçoit les données chiffrées provenant du centre de diffusion (10) et le module de gestion reçoit les messages d'autorisation (EMM) du centre de gestion (11).

WO 2004/030363 A1

SYSTÈME DE DÉCHIFFREMENT DE DONNÉES À ACCÈS CONDITIONNEL

La présente invention concerne un système de déchiffrement de données à accès conditionnel.

De tels systèmes sont notamment utilisés dans le domaine de la télévision numérique à péage. Dans ce cas, le flux numérique de données transmis vers le téléviseur est chiffré afin de pouvoir en contrôler l'utilisation et de définir des conditions pour une telle utilisation. Ce chiffrement est réalisé grâce à des mots de contrôle (Control Words) qui sont changés à intervalle régulier (typiquement entre 5 et 30 secondes, bien que des intervalles nettement plus longs puissent être utilisés) afin de dissuader toute attaque visant à retrouver un tel mot de contrôle.

Pour que le récepteur puisse déchiffrer le flux chiffré par ces mots de contrôle, ces derniers lui sont envoyés indépendamment du flux dans des messages de contrôle (ECM) chiffrés par une clé propre au système de transmission entre un centre de gestion et un module de sécurité de l'unité d'utilisateur. En effet, les opérations de sécurité sont effectuées dans un module de sécurité (SC) qui est généralement réalisé sous la forme d'une carte à puce, réputée inviolable. Ce module peut être soit de type amovible soit directement intégré au récepteur.

Lors du déchiffrement d'un message de contrôle (ECM), il est vérifié, dans le module de sécurité (SC), que le droit pour accéder au flux considéré est présent. Ce droit peut être géré par des messages d'autorisation (EMM) qui chargent un tel droit dans le module de sécurité. D'autres possibilités sont également envisageables telles que l'envoi de clés de déchiffrement.

Pour la suite de l'exposé, on appellera "événement" un contenu vidéo, audio (par exemple MP3) ou données (programme de jeu par exemple) qui est chiffré selon la méthode connue des mots de contrôle, chaque

événement pouvant être chiffré par un ou plusieurs mots de contrôle, chacun ayant une durée de validité déterminée.

La comptabilisation de l'utilisation de tels événements est aujourd'hui basée sur le principe de l'abonnement, de l'achat d'événements ou du paiement par unité de temps.

L'abonnement permet de définir un droit associé à un ou des canaux de diffusion transmettant ces événements et permet à l'utilisateur d'obtenir ces canaux en clair si le droit est présent dans son module de sécurité.

Parallèlement, il est possible de définir des droits propres à un événement, tel qu'un film ou un match de football. L'utilisateur peut acquérir ce droit (achat par exemple) et cet événement sera spécifiquement géré par ce droit. Cette méthode est connue sous l'appellation "pay-per-view" (PPV).

Pour ce qui concerne le paiement par unité de temps, le module de sécurité comprend un crédit qui est débité en fonction de la consommation réelle de l'utilisateur. Ainsi par exemple, une unité sera débitée chaque minute à ce crédit quel que soit le canal ou l'événement regardé. Il est possible selon les implémentations techniques, de varier l'unité de comptabilisation, soit dans la durée, soit dans la valeur du temps alloué, voire en combinant ces deux paramètres pour adapter la facturation au type d'événement transmis.

Un message de contrôle (ECM) ne contient pas uniquement le mot de contrôle, mais également les conditions pour que ce mot soit renvoyé au récepteur/décodeur. Lors du déchiffrement des mots de contrôle, il sera vérifié si un droit associé aux conditions d'accès énoncées dans le message est présent dans le module de sécurité.

Le mot de contrôle n'est retourné à l'unité d'utilisateur que lorsque la comparaison est positive. Ce mot de contrôle est contenu dans un message de contrôle ECM qui est chiffré par une clé de transmission.

Pour que le droit soit présent dans le module de sécurité, il est généralement chargé dans ce module par un message d'autorisation (EMM) qui pour des raisons de sécurité, est généralement chiffré par une clé différente dite clé de droit (RK).

Selon une forme connue de diffusion de télévision à péage, les trois éléments suivants sont nécessaires pour déchiffrer un événement à un moment donné:

- les données relatives à l'événement chiffré par un ou une pluralité de mots de contrôle (CW),

- le ou les messages de contrôle ECM contenant les mots de contrôle (CW) et les conditions d'accès (AC)

- le droit correspondant stocké dans le module de sécurité permettant de vérifier les dites conditions d'accès.

Les systèmes de déchiffrement du type décrit ci-dessus sont actuellement tous formés d'équipements relativement grands. Ils sont reliés à un dispositif d'exploitation ou de visualisation tel que par exemple une télévision au moyen d'un câble. Ils ne sont pas prévus pour pouvoir être déplacés facilement. Il n'est donc pas possible de déplacer son propre décodeur et de le raccorder simplement sur une autre télévision, et d'acquérir des droits ponctuels. De plus, dans les systèmes actuels, relativement peu d'installations ont une ligne de retour permettant de communiquer depuis le décodeur vers un centre de gestion. Les installations qui ont une ligne de retour n'ont généralement pas d'interface permettant de communiquer de façon conviviale avec ce centre de gestion. En effet, les lignes de retour sont prévues pour une communication entre le décodeur et le centre de gestion, mais pas entre l'utilisateur et ce centre. Il est ainsi malaisé d'acquérir des droits ponctuels de façon rapide et simple. De plus, dans tous les systèmes connus, les flux contenant les données,

les messages de contrôle et les messages d'autorisation proviennent d'une source unique qui gère ses propres abonnements, sans pouvoir offrir une gamme d'abonnements de différentes sources.

La communication avec un centre de gestion a été améliorée dans des systèmes permettant de charger des droits ponctuels. Un tel système est décrit dans le brevet américain US 5,901,339. Ce document décrit un système comportant plusieurs centres de diffusion de données ou d'événements chiffrés, destinés à transmettre ces événements à un système d'exploitation tel qu'un téléviseur ou un autre moyen d'affichage. Ces événements sont associés d'une part à un numéro d'identification unique et d'autre part à un code de déchiffrement. Le système comprend également un centre de chargement auquel sont transmis, avant la diffusion des événements, le numéro d'identification de chaque événement, associé au code de déchiffrement. Lorsqu'un utilisateur souhaite acquérir des droits pour déchiffrer un événement chiffré, il appelle le centre de chargement au moyen d'un appareil de communication tel qu'un téléphone, et indique le numéro d'identification de l'événement qu'il veut acquérir. Le centre de chargement transmet à l'appareil de communication, le code de déchiffrement de l'événement considéré. A son tour, l'appareil de chargement transmet ce code au décodeur de l'utilisateur. Lorsque l'événement est diffusé, le décodeur possède le code de déchiffrement et l'événement peut être déchiffré et visionné.

Ce système implique un certain nombre de contraintes. En particulier, comme le code de déchiffrement est reçu sur demande de l'utilisateur, il n'est pas commode d'utiliser plusieurs codes pour un même événement. Ce code doit rester le même pendant toute la durée de cet événement. Ceci présente un inconvénient du point de vue de la sécurité. A titre de comparaison, dans les systèmes actuels, les mots de contrôle utilisés pour le chiffrement et de déchiffrement d'événements sont changés à des intervalles qui peuvent varier de 2 à 30 secondes environ.

Dans le système selon US 5,901,339, plusieurs centres de diffusion sont connectés à un seul centre de chargement. Cela implique notamment que tous les diffuseurs doivent placer leurs moyens cryptographiques dans le même centre de chargement, ce qui n'est pas optimal du point de vue sécuritaire.

Ce système présente également d'autres défauts relatifs à la sécurité. D'une part, la transmission du code de déchiffrement entre le centre de chargement et le décodeur de l'utilisateur se fait au moyen d'une ligne téléphonique via un téléphone sans moyen de sécurité. Cela implique qu'il est relativement aisé d'obtenir ce code de façon illégale et de l'utiliser en relation avec un autre décodeur. D'autre part, comme le centre de chargement ne dispose d'aucune information concernant le décodeur qui demande le code de déchiffrement, il est possible d'utiliser ce code sur n'importe quel décodeur. Cela signifie qu'une fois acquis en toute légalité, le code de déchiffrement peut être facilement transmis à d'autres décodeurs pour déchiffrer illégalement un événement ou des données.

Le document "EBU Technical Review" Winter 1995 N°. 266 intitulé "Functional model of a conditional access system" décrit différentes variantes de systèmes à accès conditionnel destinés notamment à la télévision à péage, ces systèmes utilisant un déchiffrement à deux niveaux, à savoir un premier niveau sécurisé au moyen de messages de contrôle ECM et un deuxième niveau utilisant des messages d'autorisation EMM. Dans l'une de ces variantes, le système à accès conditionnel est destiné à être utilisé simultanément par plusieurs diffuseurs de données à accès conditionnel. Le système tel que décrit comporte notamment un système de gestion des droits, en charge de générer et d'envoyer les messages d'autorisation EMM, et un système de gestion d'autorisations en charge de générer des mots de contrôle pour le chiffrement des données des diffuseurs.

Dans tous les exemples représentés et décrits dans ce document, chaque diffuseur est associé de façon univoque à un système de gestion des droits. Il n'est pas possible d'associer un seul diffuseur à plusieurs systèmes de gestion de droits. Dans le système selon ce document, le fait d'utiliser un ou plusieurs fournisseurs de services est totalement transparent pour l'utilisateur. En effet, celui-ci ne peut pas choisir un opérateur ou un autre, il peut uniquement choisir un service, qu'il y ait un ou plusieurs opérateurs.

Ce système ne permet pas de résoudre les problèmes liés au déplacement simple du décodeur et à l'acquisition de droits ponctuels, ni le problème de communication entre l'utilisateur et le centre de gestion.

La présente invention se propose de pallier les inconvénients des systèmes de l'art antérieur et de réaliser un système qui puisse facilement être déplacé et utilisé sur pratiquement n'importe quel dispositif d'exploitation adapté. De plus, un tel système simplifie la gestion des droits d'accès au niveau du centre de diffusion et offre une plus grande souplesse à l'utilisateur tout en garantissant une sécurité optimale telle que les informations obtenues par un utilisateur et destinées à un décodeur déterminé ne peuvent pas être utilisées sur un autre décodeur.

Ces buts sont atteints par un système de déchiffrement de données à accès conditionnel, ce système mettant en œuvre :

- un centre de diffusion agencé pour diffuser des données chiffrées par au moins un mot de contrôle,
- au moins un centre de gestion agencé pour diffuser des messages personnels relatifs à la gestion des moyens d'accès aux données chiffrées,
- un dispositif d'exploitation destiné à rendre utilisables lesdites données chiffrées, et

- un décodeur agencé pour déchiffrer au moins une partie des données chiffrées, placé entre le centre de diffusion et le dispositif d'exploitation,

caractérisé en ce que

- le décodeur est formé d'un module de réception et de déchiffrement des données chiffrées et d'un module de gestion des droits d'accès à ces données, ces modules étant physiquement distincts, le module de réception étant connecté au dispositif d'exploitation et le module de gestion étant agencé pour communiquer avec le module de réception,
- en ce que le module de gestion comporte un module de sécurité comprenant un numéro d'identification unique et des données permettant de sécuriser la liaison entre ledit centre de gestion et le module de sécurité, ce module de sécurité étant agencé pour vérifier le contenu des messages personnels et pour permettre ou empêcher le déchiffrement du ou des mots de contrôle en fonction du contenu des messages personnels,
- et en ce que le module de réception reçoit les données chiffrées provenant du centre de diffusion via une première voie de communication, et le module de gestion reçoit les messages personnel par le centre de gestion via une deuxième voie de communication.

La présente invention et ses avantages seront mieux compris en référence à la description de différents modes de réalisation et aux dessins annexés, dans lesquels :

- la figure 1 représente une vue d'ensemble d'un premier mode de réalisation du système selon la présente invention; et
- la figure 2 est une vue d'ensemble d'un deuxième mode de réalisation de l'invention.

En référence à ces figures, le système de l'invention comporte essentiellement un centre de diffusion 10 agencé pour diffuser des données chiffrées, au moins un centre de gestion 11 agencé pour diffuser des messages d'autorisation (EMM) et traiter la gestion de droits d'accès aux données chiffrées, un dispositif d'exploitation 12 destiné à rendre utilisables, ces données chiffrées et un décodeur 13 agencé pour déchiffrer au moins une partie des données chiffrées.

Le centre 10 de diffusion de données chiffrées peut être un dispositif classique par câble ou par satellite notamment. Ce centre émet des données sous forme chiffrées. La nature de ces données dépend bien entendu de l'utilisation qui doit en être faite. Dans la suite du texte, il est supposé que les données sont utilisées dans un système de télévision à accès conditionnel. Les données sont donc formées d'un contenu vidéo CT, c'est-à-dire des images et du son. D'autres données spécifiques à l'utilisation peuvent également être inclues, de façon bien connue de l'homme du métier. Ces données, ou au moins une partie d'entre elles, sont chiffrées au moyen de mots de contrôle et sont notées cw(CT) sur les figures.

Selon une première forme de réalisation, les mots de contrôle cw sont transmis, sous forme chiffrée, par le centre de diffusion en même temps que les données chiffrées. Selon une autre forme de réalisation, ces mots de contrôle peuvent être diffusés par le centre de gestion 11 du fait que l'encryption du message de contrôle, comprenant le mot de contrôle, est spécifiquement géré selon un protocole propre à chaque centre de gestion.

L'appellation "message personnel" représente un message d'autorisation (EMM) dans le cas où les messages de contrôle (ECM) sont non spécifiques, ces messages personnels permettant l'accès aux données par la mise en mémoire d'un droit. Le mot de contrôle est extrait de ce message et envoyé au module de réception généralement sous forme

chiffrée, de sorte que les mots de contrôle ne peuvent pas être copiés à ce niveau et envoyés à un autre utilisateur.

Le ou plus généralement les centres de gestion 11 sont chargés de gérer les droits d'accès aux données. Ils peuvent chacun gérer des types de droits différents, notamment des abonnements, des accès ponctuels, des bouquets de programmes différents. Pour réaliser ceci, ils diffusent également les messages d'autorisation (EMM) correspondants, à destination des décodeurs concernés.

Le dispositif d'utilisation 12 est également bien entendu adapté aux données à transmettre. Dans le cas choisi de la télévision à accès conditionnel, le dispositif d'exploitation est un téléviseur.

Le décodeur 13 comporte un module de réception et de déchiffrement 14 des données et un module de gestion 15 des droits d'accès à ces données. Le module de gestion des droits est réalisé de telle façon qu'il soit aisément portable. Il peut judicieusement être réalisé au moyen d'un téléphone portable. Le module de gestion comporte également un module de sécurité 16. Ce module de réception et de déchiffrement peut comprendre des moyens de communication standardisé avec le module de gestion. Ainsi, le module de réception est capable de dialoguer avec n'importe quel module de gestion.

Un module de sécurité évolué peut comprendre des zones mémoires propres à chaque centre de gestion. Dans le cas d'un téléphone portable, l'opérateur de téléphonie peut allouer des zones mémoires qui seront ensuite initialisée par des paramètres propres à chaque centre de gestion. Ces paramètres sont par exemple une clé de décryption des messages d'autorisation (EMM), l'identification de l'abonné selon le système propre audit centre de gestion, voire un crédit.

Dans le cas où des opérateurs différents ne souhaitent pas intégrer leur sécurité sur un module commun, ou simplement pour augmenter la souplesse d'utilisation, il est possible de prévoir une connectique permettant soit de changer facilement de module de sécurité, soit d'en utiliser plusieurs à la fois. Ces modules peuvent être réalisés sous la forme d'une carte à puce coopérant avec un lecteur approprié du module de gestion ou sous une forme plus compacte permettant la mise en place de plusieurs modules de sécurité simultanément. Dans ce cas, chaque puce gère les autorisations provenant de l'un des centres de gestion.

Il est également possible de prévoir une carte ou un autre support comportant plusieurs puces, chacune d'elles gérant les autorisations provenant de l'un des centres de gestion. Un tel module de sécurité est illustré par la figure 2, sous la référence 16.

Le module de sécurité, ou chacun des modules lorsqu'il y en a plusieurs, contient un numéro d'identification unique (UA) et des données propres aux centres de gestion 11 avec lesquels ces modules sont autorisés à communiquer. Cela signifie qu'avant de pouvoir obtenir et déchiffrer un message d'autorisation (EMM) provenant d'un centre de gestion, les données relatives à ce centre de gestion doivent avoir été préalablement chargées dans le module de sécurité. Les données propres au centre de gestion sont par exemple une clé de chiffrement ou un code permettant de former une clé de chiffrement, ces données permettant de sécuriser la liaison entre le centre de gestion et le module de sécurité. Selon un mode de réalisation avantageux, les messages d'autorisation EMM sont envoyés au module de sécurité sous forme chiffrée au moyen d'une clé qui dépend à la fois du centre de gestion concerné et du numéro d'identification unique UA de ce module de sécurité. De cette manière, un message d'autorisation reçu par un module de sécurité ne pourra pas être utilisé par un autre module. De plus, un module falsifié, ne contenant pas les données propres

au centre de gestion ne pourra pas utiliser le message d'autorisation puisqu'il ne sera pas capable de le déchiffrer.

Le module de gestion 15 comporte avantageusement un lecteur de carte à puce destiné à être utilisé avec une carte de crédit ou une carte à prépaiement 17. De cette façon, la gestion des paiements est assurée lorsqu'un évènement est commandé. Ceci permet en outre d'utiliser le module de gestion comme porte-monnaie électronique. Une telle carte est illustrée sous la référence 17 dans la figure 2.

Selon un mode de réalisation mettant en œuvre plusieurs centres de gestion pour les données diffusées vers le module de réception, il est prévu d'adjoindre aux dites données chiffrées des informations descriptives pour permettre à l'utilisateur de se connecter sur le centre de gestion approprié. Ces informations descriptives sont transmises depuis le module de réception vers le module de gestion et affichées sur ledit module. L'utilisateur peut effectuer son choix et initier une communication avec un centre, pour autant que son module de sécurité supporte les fonctions de sécurité exigées par ce centre de gestion. Ces informations descriptives, en plus de décrire le produit vidéo ou audio, comprennent une adresse de type téléphonique ou Internet. Cette adresse sera utilisée pour le dialogue en vue de l'envoi du message personnel permettant de recevoir les droits ou les clés nécessaires à l'accès aux données chiffrées.

Le module de réception et de déchiffrement 14 des données peut être intégré directement dans l'appareil de télévision 12. Dans ce cas, pour pouvoir lire des données chiffrées sur un tel téléviseur, il suffit de disposer du module de gestion 15 et des droits correspondants à l'événement souhaité. Cet événement peut donc être visualisé à partir de n'importe quel téléviseur équipé de façon adéquate. Ce mode de réalisation est illustré schématiquement par la figure 2. Selon une autre forme de réalisation avantageuse, il peut être formé d'un boîtier qui peut être connecté à la

télévision au moyen d'un câble de connexion ou directement par une sortie sur la télévision. Ceci permet d'utiliser de façon simple, la présente invention sur des téléviseurs existants.

Le système selon l'invention fonctionne de la manière suivante :

Comme mentionné précédemment, le contenu vidéo CT est diffusé par le centre de diffusion 10 de données chiffrées. Simultanément, ce premier centre diffuse également le ou les mots de contrôle cw qui ont été utilisés pour chiffrer les données. Lorsque l'on souhaite utiliser des données du système à accès conditionnel, par exemple, pour voir un événement tel qu'un film ou un match de football par exemple, pour lequel l'accès est soumis à un droit, il est tout d'abord nécessaire d'acquérir ce droit. Celui-ci peut être donné par une carte à pré-paiement disposée dans le module de gestion 15, ou il peut être chargé dans ce module grâce aux moyens de communication entre le module et l'un des centres de gestion 11, qui gère les droits d'accès.

Pour obtenir les messages d'autorisation EMM qui vont permettre le déchiffrement des mots de contrôle cw nécessaire au déchiffrement des données et donc à la visualisation de l'évènement, le module de réception et de déchiffrement 14 établi une communication avec l'un des centres de gestion. Comme mentionné précédemment, le module de réception peut être formé d'un téléphone portable. Dans ce cas, le contact est établi en composant un numéro de téléphone correspondant au centre de diffusion. Le choix de l'événement pour lequel on souhaite acquérir les droits se fait au moyen d'un "menu" préenregistré, chaque choix du menu correspondant à un numéro particulier sur le clavier du téléphone portable. Le téléchargement du message d'autorisation correspondant à l'évènement choisi se fait après avoir pressé une touche de validation sur le clavier du téléphone. Ce message d'autorisation est avantageusement chiffré au

moyen d'une clé dépendant à la fois du numéro d'identification unique UA du module de sécurité et des données propres au centre de gestion.

Le module de réception et de déchiffrement 14 est connecté au téléviseur, par exemple sur une sortie de celle-ci ou directement intégré dans le téléviseur.

Dans un premier mode de réalisation, le module de réception 14 reçoit, en provenance du premier dispositif de diffusion 10, les données chiffrées cw(CT) au moyen de mots de contrôle ainsi que les mots de contrôle cw eux-mêmes. Il reçoit également les messages d'autorisation EMM provenant d'un des centres de gestion 11. Le module de réception 14 transmet les mots de contrôle cw au module de gestion des droits. Cette transmission peut être effectuée au moyen d'ondes infrarouge ou radio par exemple. Ce module de gestion des droits vérifie qu'il a bien acquis les droits correspondants à l'événement choisi. Si tel est le cas, les messages de contrôle ECM sont traités dans le module de sécurité de façon à en extraire les mots de contrôle cw. Ceux-ci sont ensuite transmis, à une fréquence adéquate correspondant à la fréquence utilisée pour le chiffrement des données, au module de réception 14 qui les utilise alors pour déchiffrer les données et rendre ainsi visible l'événement.

Dans un deuxième mode de réalisation, illustré schématiquement par la figure 2, le flux contenant les données chiffrées, les messages de contrôle et les messages d'autorisation sont reçus par le dispositif de gestion des droits 15. Ces flux sont traités comme précédemment et les données déchiffrées sont transmises en clair au dispositif de réception.

Ce système permet de réaliser un décodeur aisément transportable et qui peut être utilisé sur n'importe quel téléviseur. Dans le cas où le module de réception des données 14 est intégré au téléviseur, il suffit de disposer du module de gestion 15 pour avoir accès à un événement. De cette façon, les contraintes pour les utilisateurs sont supprimées. En outre, le fait

d'utiliser des centres de gestion pour les messages d'autorisation, distincts du centre de diffusion des données augmente le choix offert à l'utilisateur et facilite l'emploi de systèmes à accès conditionnel.

Du fait que les mots de contrôle sont déchiffrés dans le module de gestion et transmis vers le module de réception, la communication entre ces deux modules sera de préférence sécurisée. Pour cela, il existe différentes procédures d'appariement habituellement adaptées au couple formé par l'unité de sécurité et le décodeur. Dans notre cas, ces procédures sont appliquées entre le module de réception et le module de gestion. Un exemple de ce type d'appariement est décrit dans la demande WO 02/052515.

Pour garantir que les mots de contrôle ne sont pas disséminés vers d'autres modules de réception et de déchiffrement, et dans un schéma à deux niveaux c'est-à-dire lorsque le message de contrôle est de type personnel, le centre de gestion peut requérir une clé de chiffrement propre au module de déchiffrement. Cette clé est directement codée dans le module de déchiffrement et est unique pour chaque module.

Dans le cas où les messages de contrôle ECM contenant les mots de contrôle cw sont envoyés par le centre de gestion, ou dans le cas similaire où un événement est chiffré au moyen d'une seule clé qui est envoyée au module de sécurité par un centre de gestion, ce centre de gestion applique, sur un mot de contrôle donné, une encryption propre à la clé unique du module de déchiffrement, puis une encryption propre au système de télécommunication entre le centre de gestion et le module de sécurité au module de sécurité du module de gestion. Ainsi, si ce message était intercepté par un module de sécurité falsifié, le mot de contrôle obtenu serait inutilisable pour un autre module de déchiffrement car encore encrypté par la clé unique de ce module.

Selon un mode de réalisation, la liaison entre le module de gestion et le centre de gestion est une liaison point à point sécurisée. Il est dès lors possible de transmettre des commandes en relation avec les images et événements diffusés par le centre de diffusion. Cette fonction est utilisée pour placer des commandes via le module de gestion ou des réponses à des interrogations.

Dans une forme d'application, les images diffusées vers le décodeur sont des images réelles provenant de jeux de casino tels que la roulette, le black jack et le possesseur d'un tel module de gestion peut d'une manière interactive et en temps réel, jouer là où il se trouve. Les moyens de sécurité mis en place pour l'accès conditionnel aux données télédiffusées peuvent également être utilisées pour ce type d'application. Dans ce type d'application, le casino est relié au centre de gestion pour déterminer l'identité du porteur du module de gestion ou tout au moins que ce porteur soit solvable. Le centre de gestion alloue un crédit à ce porteur et communique cette information au casino.

REVENDICATIONS

1. Système de déchiffrement de données à accès conditionnel, ce système mettant en œuvre :

- un centre de diffusion (10) agencé pour diffuser des données chiffrées par au moins un mot de contrôle (cw),
- au moins un centre de gestion (11) agencé pour diffuser des messages personnels (ECM, EMM) relatifs à la gestion des moyens d'accès aux données chiffrées,
- un dispositif d'exploitation (12) destiné à rendre utilisables lesdites données chiffrées, et
- un décodeur (13) agencé pour déchiffrer au moins une partie des données chiffrées, placé entre le centre de diffusion (10) et le dispositif d'exploitation (12),

caractérisé en ce que

- le décodeur (13) est formé d'un module de réception et de déchiffrement (14) des données chiffrées et d'un module de gestion (15) des droits d'accès à ces données, ces modules étant physiquement distincts, le module de réception (14) étant connecté au dispositif d'exploitation (12) et le module de gestion (15) étant agencé pour communiquer avec le module de réception,
- en ce que le module de gestion (15) comporte un module de sécurité (16) comprenant un numéro d'identification unique (UA) et des données permettant de sécuriser la liaison entre ledit centre de gestion (11) et le module de sécurité (16), ce module de sécurité étant agencé pour vérifier le contenu des messages personnels (ECM, EMM) et pour permettre ou empêcher le déchiffrement du ou des mots de contrôle (cw) en fonction du contenu des messages personnels,

- et en ce que le module de réception (14) reçoit les données chiffrées provenant du centre de diffusion (10) via une première voie de communication, et le module de gestion (15) reçoit les messages personnel (ECM, EMM) par le centre de gestion (11) via une deuxième voie de communication.

2. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que la communication entre le module de réception (14) et le module de gestion (15) est une communication par ondes.

3. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que le module de gestion (15) des droits est un téléphone portable.

4. Système de déchiffrement de données selon la revendication 3, caractérisé en ce que le module de sécurité (16) comprend des fonctions d'identification nécessaires à la téléphonie, et au moins une zone mémoire propre à un centre de gestion (11), cette zone comprenant les paramètres de sécurité pour la réception des messages d'autorisation (EMM) dudit centre de gestion.

5. Système selon les revendications 1 à 4, caractérisé en ce que le centre de diffusion (10) est agencé pour diffuser des messages de contrôle (ECM) comprenant le ou les mots de contrôle (cw), et en ce que les messages personnels diffusés par le centre de gestion (11) correspondent à un message d'autorisation (EMM).

6. Système selon les revendications 1 à 4, caractérisé en ce que le centre de gestion (11) est agencé pour diffuser des messages personnels comprenant le ou les mots de contrôle (cw), le module de sécurité (16) du module de gestion (15) disposant des moyens pour déterminer si ce message lui est destiné et de moyens pour transmettre ce mot de contrôle (cw) au module de réception (14).

7. Système selon la revendication 6, caractérisé en ce que le module de réception et de déchiffrement (14) comprend une clé unique de décryption appliquée au mot de contrôle (cw), cette clé servant à encrypter les mots de contrôle au centre gestion (11) avant leur transmission vers le module de gestion (15).

8. Système de déchiffrement de données selon la revendication 1, comportant au moins deux centres de gestion (11), caractérisé en ce que le module de sécurité (16) du module de gestion (15) comporte des paramètres de sécurité pour la réception des messages d'autorisation (EMM) provenant de centres de gestion (11) distincts.

9. Système de déchiffrement de données selon les revendications 1 à 8, le centre de diffusion (10) étant agencé pour transmettre des informations descriptives des données chiffrées, caractérisé en ce que ces données contiennent des indications nécessaires à l'établissement d'une communication avec le centre de gestion (11) en charge de l'autorisation de ces données, et sont transmises au module de gestion (15), ce dernier étant agencé pour établir une communication avec le centre de gestion (11) concerné pour l'obtention du message d'autorisation (EMM) .

10. Système de déchiffrement de données selon l'une des revendications précédentes, caractérisé en ce que le module de réception et de déchiffrement (14) est intégré dans le dispositif d'exploitation (12).

11. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que le module de réception et de déchiffrement (14) comprend des moyens de communication standardisé avec le module de gestion (15) de sorte qu'un module de réception et de déchiffrement (14) puisse dialoguer avec une pluralité de modules de gestion (15).

12. Système de déchiffrement de données selon l'une des revendications précédentes, caractérisé en ce que le module de gestion

(15) comprend des moyens pour établir une clé d'appariement avec le module de réception (14), cette clé étant destinée à encrypter et décrypter au moins le ou les mots de contrôle (cw) transmis du module de gestion (15) vers le module de réception (14).

5

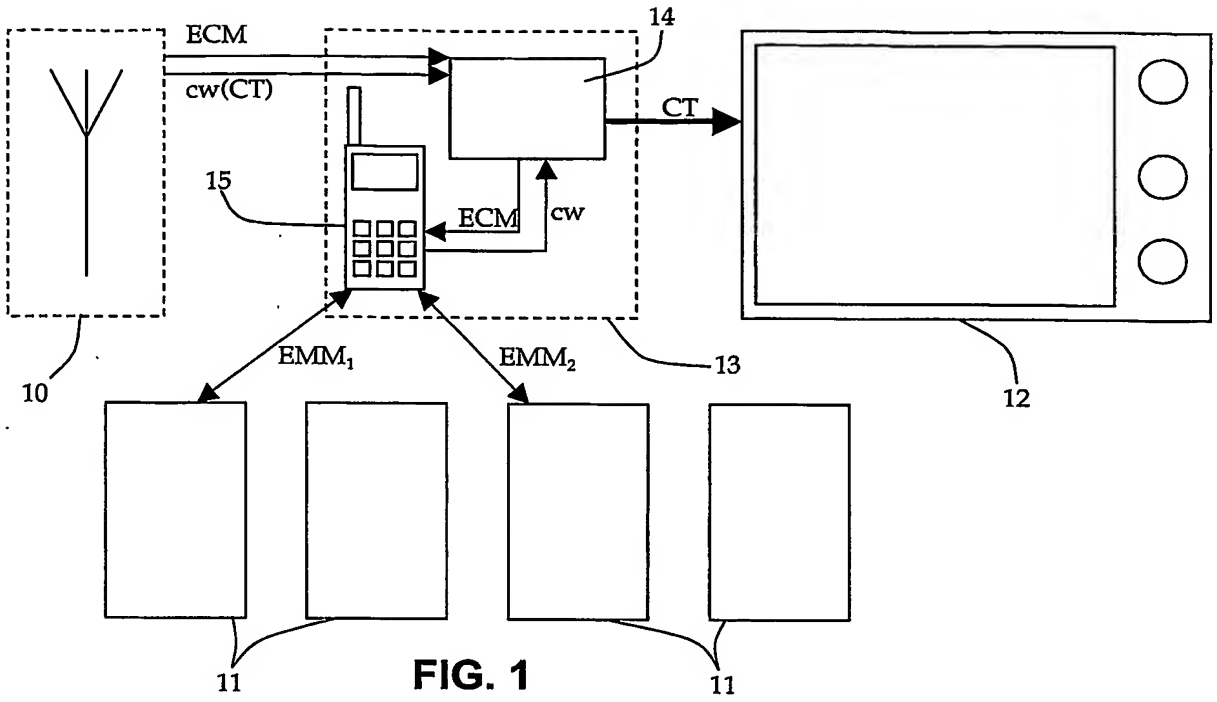
ECM
cw(CT)
14
CT
15
ECM
cw
EMM1
EMM2
10
13
12
11
11

FIG. 1

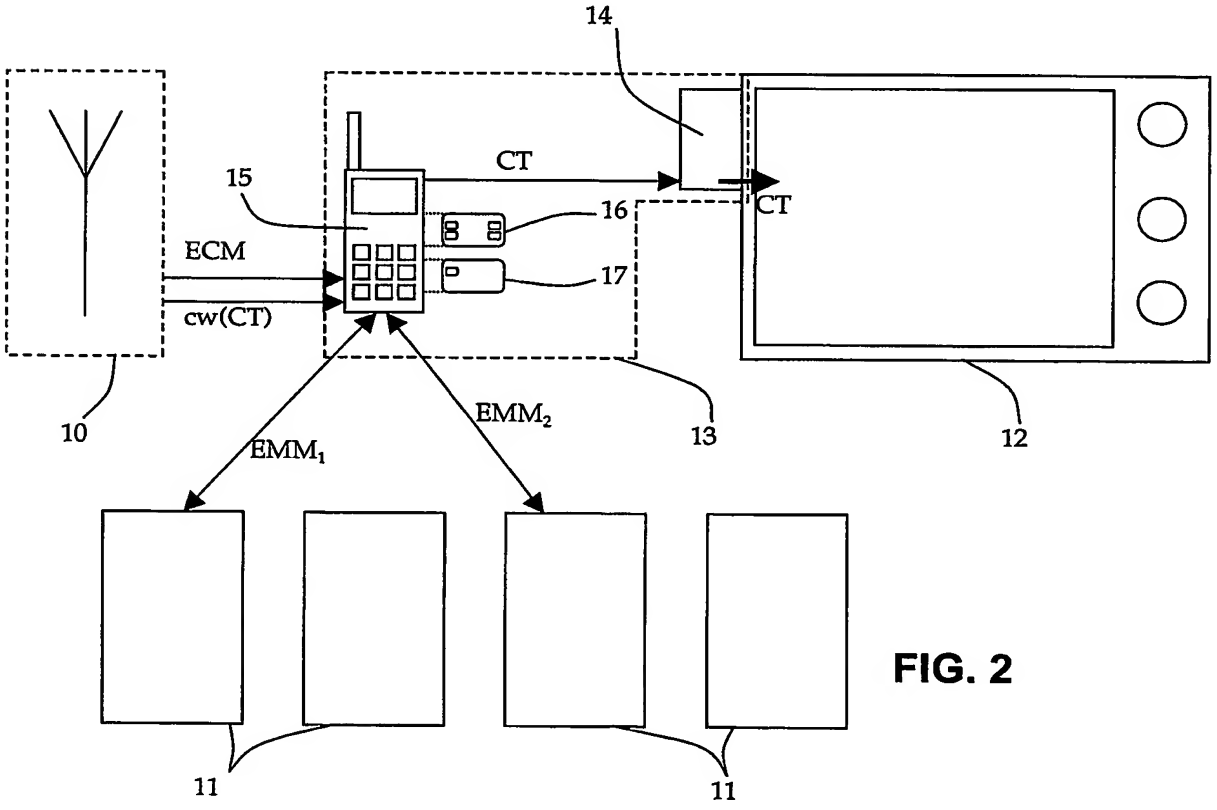
14
CT
15
16
CT
ECM
17
cw(CT)
10
13
12
EMM2
EMM1
11
11

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB 03/04121

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04N5/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	VAN RIJNSOEVER B J ET AL: "Interoperable content protection for digital TV" MULTIMEDIA AND EXPO, 2000. ICME 2000. 2000 IEEE INTERNATIONAL CONFERENCE ON NEW YORK, NY, USA 30 JULY-2 AUG. 2000, PISCATAWAY, NJ, USA,IEEE, US, 30 July 2000 (2000-07-30), pages 1407-1410, XP010512769 ISBN: 0-7803-6536-4 the whole document -/--	1-12

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 December 2003	23/12/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fantini, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internation ation No
PCT/IB 03/04121

C.(Continuation) DOCUMENTS CONS[redacted]O TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 901 339 A (SAITO MAKOTO) 4 May 1999 (1999-05-04) abstract column 2, line 19 - line 31 column 3, line 23 - line 56 column 4, line 16 - line 42 column 13, line 28 - line 33 figures 1,2	1-12
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, no. 266, 21 December 1995 (1995-12-21), pages 64-77, XP000559450 ISSN: 0251-0936 paragraph '0002! paragraph '03.1! paragraph '03.4! paragraph '05.1! paragraph '05.2! paragraph '5.3.1! paragraph '07.2! paragraph '7.2.1! figures 3,6	1-12
A	WO 02/21835 A (ROBINSON WILLIAM NEIL ;MOTOROLA INC (US)) 14 March 2002 (2002-03-14) abstract page 2, line 1 - line 11 page 12, line 13 - line 22 figure 2	1-12
A	WO 02/052515 A (NAGRAVISION SA ;SASSELLI MARCO (CH); JAQUIER JEAN-LUC (CH)) 4 July 2002 (2002-07-04) abstract page 2, line 1 - line 14 page 3, line 8 - line 12 page 4, line 17 - page 5, line 3	1-12
A	EP 1 182 874 A (CANAL & TECHNOLOGIES SA) 27 February 2002 (2002-02-27) page 2, line 1 - line 21 page 2, line 45 - line 51 page 3, line 12 - line 16 page 3, line 28 - line 39 page 9, line 21 - line 44 page 10, line 19 - page 11, line 36 page 14, line 10 - line 32 figure 2	1-12

-/--

INTERNATIONAL SEARCH REPORT

Internation[illegible]cation No
PCT/IB 03/04121

C.(Continuation) DOCUMENTS CONSID[illegible]TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 111 923 A (IRDETO ACCESS BV) 27 June 2001 (2001-06-27) column 1, line 1 - line 17 column 3, line 31 - column 4, line 36	1-12

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internatior ation No
PCT/IB 03/04121

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5901339	A	04-05-1999	JP	6141004 A	20-05-1994
			US	5794115 A	11-08-1998
			DE	4335835 A1	09-06-1994
			FR	2697707 A1	06-05-1994
			GB	2272823 A ,B	25-05-1994
			GB	2295947 A ,B	12-06-1996
			GB	2305832 A ,B	16-04-1997
			HK	1001941 A1	17-07-1998
			HK	1001946 A1	17-07-1998
			HK	1002721 A1	11-09-1998
			US	5504933 A	02-04-1996
WO 0221835	A	14-03-2002	GB	2366942 A	20-03-2002
			AU	2353002 A	22-03-2002
			WO	0221835 A1	14-03-2002
WO 02052515	A	04-07-2002	BR	0116360 A	02-12-2003
			CA	2432092 A1	04-07-2002
			CA	2432593 A1	04-07-2002
			EP	1344195 A1	17-09-2003
			EP	1368716 A2	10-12-2003
			WO	02052515 A1	04-07-2002
			WO	02052389 A2	04-07-2002
			US	2003135747 A1	17-07-2003
			US	2003135471 A1	17-07-2003
EP 1182874	A	27-02-2002	EP	1182874 A1	27-02-2002
			AU	9020701 A	04-03-2002
			CA	2420795 A1	28-02-2002
			EP	1332621 A2	06-08-2003
			WO	0217635 A2	28-02-2002
			US	2003182579 A1	25-09-2003
EP 1111923	A	27-06-2001	EP	1111923 A1	27-06-2001
			AU	4049501 A	03-07-2001
			BR	0008324 A	29-01-2002
			CA	2364398 A1	28-06-2001
			CN	1357197 T	03-07-2002
			WO	0147271 A2	28-06-2001
			EP	1238537 A2	11-09-2002
			HU	0200126 A2	29-05-2002
			JP	2003518843 T	10-06-2003
			NZ	513568 A	28-11-2003
			US	2002126847 A1	12-09-2002
			ZA	200106073 A	19-12-2002

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/IB 03/04121

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/167 H04N5/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	VAN RIJNSOEVER B J ET AL: "Interoperable content protection for digital TV" MULTIMEDIA AND EXPO, 2000. ICME 2000. 2000 IEEE INTERNATIONAL CONFERENCE ON NEW YORK, NY, USA 30 JULY-2 AUG. 2000, PISCATAWAY, NJ, USA,IEEE, US, 30 juillet 2000 (2000-07-30), pages 1407-1410, XP010512769 ISBN: 0-7803-6536-4 le document en entier	1-12

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
15 décembre 2003	23/12/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fantini, F

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES C[illegible] PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
Y	US 5 901 339 A (SAITO MAKOTO) 4 mai 1999 (1999-05-04) abrégé colonne 2, ligne 19 - ligne 31 colonne 3, ligne 23 - ligne 56 colonne 4, ligne 16 - ligne 42 colonne 13, ligne 28 - ligne 33 figures 1,2	1-12
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, no. 266, 21 décembre 1995 (1995-12-21), pages 64-77, XP000559450 ISSN: 0251-0936 alinéa '0002! alinéa '03.1! alinéa '03.4! alinéa '05.1! alinéa '05.2! alinéa '5.3.1! alinéa '07.2! alinéa '7.2.1! figures 3,6	1-12
A	WO 02/21835 A (ROBINSON WILLIAM NEIL ;MOTOROLA INC (US)) 14 mars 2002 (2002-03-14) abrégé page 2, ligne 1 - ligne 11 page 12, ligne 13 - ligne 22 figure 2	1-12
A	WO 02/052515 A (NAGRAVISION SA ;SASSELLI MARCO (CH); JAQUIER JEAN-LUC (CH)) 4 juillet 2002 (2002-07-04) abrégé page 2, ligne 1 - ligne 14 page 3, ligne 8 - ligne 12 page 4, ligne 17 - page 5, ligne 3	1-12
A	EP 1 182 874 A (CANAL & TECHNOLOGIES SA) 27 février 2002 (2002-02-27) page 2, ligne 1 - ligne 21 page 2, ligne 45 - ligne 51 page 3, ligne 12 - ligne 16 page 3, ligne 28 - ligne 39 page 9, ligne 21 - ligne 44 page 10, ligne 19 - page 11, ligne 36 page 14, ligne 10 - ligne 32 figure 2	1-12

-/--

RAPPORT DE RECHERCHE INTERNATIONALE

Demande I[illegible]nale No
PCT/IB 03/04121

C.(suite) DOCUMENTS CONSIDERES C[illegible] PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	EP 1 111 923 A (IRDETO ACCESS BV) 27 juin 2001 (2001-06-27) colonne 1, ligne 1 - ligne 17 colonne 3, ligne 31 - colonne 4, ligne 36	1-12

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande I onale No
PCT/IB 03/04121

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 5901339	A	04-05-1999	JP	6141004 A	20-05-1994
			US	5794115 A	11-08-1998
			DE	4335835 A1	09-06-1994
			FR	2697707 A1	06-05-1994
			GB	2272823 A ,B	25-05-1994
			GB	2295947 A ,B	12-06-1996
			GB	2305832 A ,B	16-04-1997
			HK	1001941 A1	17-07-1998
			HK	1001946 A1	17-07-1998
			HK	1002721 A1	11-09-1998
			US	5504933 A	02-04-1996
WO 0221835	A	14-03-2002	GB	2366942 A	20-03-2002
			AU	2353002 A	22-03-2002
			WO	0221835 A1	14-03-2002
WO 02052515	A	04-07-2002	BR	0116360 A	02-12-2003
			CA	2432092 A1	04-07-2002
			CA	2432593 A1	04-07-2002
			EP	1344195 A1	17-09-2003
			EP	1368716 A2	10-12-2003
			WO	02052515 A1	04-07-2002
			WO	02052389 A2	04-07-2002
			US	2003135747 A1	17-07-2003
			US	2003135471 A1	17-07-2003
EP 1182874	A	27-02-2002	EP	1182874 A1	27-02-2002
			AU	9020701 A	04-03-2002
			CA	2420795 A1	28-02-2002
			EP	1332621 A2	06-08-2003
			WO	0217635 A2	28-02-2002
			US	2003182579 A1	25-09-2003
EP 1111923	A	27-06-2001	EP	1111923 A1	27-06-2001
			AU	4049501 A	03-07-2001
			BR	0008324 A	29-01-2002
			CA	2364398 A1	28-06-2001
			CN	1357197 T	03-07-2002
			WO	0147271 A2	28-06-2001
			EP	1238537 A2	11-09-2002
			HU	0200126 A2	29-05-2002
			JP	2003518843 T	10-06-2003
			NZ	513568 A	28-11-2003
			US	2002126847 A1	12-09-2002
			ZA	200106073 A	19-12-2002